Mobile Device and Remote Working Code of Practice

Executive Summary

Leeds Beckett University recognises that it is necessary for staff to have access to mobile devices to work effectively. This CoP outlines the requirements for the use of university allocated mobile devices and remote working to ensure the continued security of the University IT Environment.

Such use must comply with this CoP to;

- ensure that the security of the University IT Environment is maintained.
- ensure that the University complies with its legal and statutory obligations.
- protect the interests of users of the University IT Environment.

CoP Statement

1. Leeds Beckett University supplies IT equipment to University users for the conducting of University business.

2. The use of mobile devices and remote working creates issues that need to be addressed, particularly around cyber security. For example, by their nature mobile devices are more susceptible to loss or theft, particularly when used in public or other non-secure locations.

3. It is essential that mobile devices are secured in accordance with professional best practice and with statutory, regulatory, and contractual requirements around cyber security.

Purpose

4. The purpose of this document is to prevent the compromise of mobile device security, and by extension the security of the University IT Environment, both within University premises and when being used for remote working.

Scope and Application

5. This CoP applies to all employees, contractors, academics, students, and any other individuals who use mobile devices to access the University IT Environment, both within university premises and when working remotely.

6. When using non-University owned devices, it is the responsibility of remote users to ensure that all reasonable measures have been taken to secure these devices. For further information refer to the Bring Your Own Device (BYOD) CoP.

7. For mobile devices not allocated by the university, please see the BYOD CoP.

8. All applicable users are required to familiarise themselves with this CoP and comply with its requirements.

9. Failure of university users to comply with this CoP may lead to the instigation of disciplinary procedures up to and including dismissal and, in certain circumstances, legal action may be taken.

10. Failure of other users to comply may lead to revocation of access, the cancellation of a contract and, in certain circumstances, legal action.

11. Completion of the University's Cyber Security Training module is required by all users to support the effective implementation of this CoP.

Standards

12. Use of the University IT Environment is subject to law and regulation, and the University seeks to ensure compliance with these via this CoP.

13. The CoP also supports adherence to standards required for University PCI DSS accreditation (this being the technical and operational requirements for processing credit card data) and Cyber Essentials (this being a standard for information security).

DEFINITIONS

14. BYOD – Bring Your Own Device. Refers to any IT device that is not owned, procured or configured by the University.

15. University IT Environment - includes all servers and clients, network connectivity, systems and application software, internal and external services, data, and other computer subsystems and components that are owned or provided by the University, or which are under the University's responsibility.

16. IT devices – This includes laptops, smart phones, tablets, USB memory sticks, digital cameras, and any other similar electronic devices.

17. University user – any individual afforded access to the University IT Environment via a direct relationship with the university e.g. students, members of staff, academics, associates.

18. PIN – Personal Identification Number

19. MFA – Multi-Factor Authentication. This is where a form of authentication is required in addition to username and password before access is granted. This could be a prompt sent

via an authenticator app installed on your phone or a one-time code that must be inputted into an authenticator app.

20. Remote Working - the practice of an employee working at their home, or in some other place that is not an organisation's usual place of business.

RESPONSIBILITIES

Responsibilities and application of the CoP

21. The Vice Chancellor is responsible for ensuring that all necessary resources are available to support the implementation of this CoP across the University.

22. The Director of Digital Services is responsible for the operational coordination of the CoP and for ensuring appropriate policies, procedures, guidance, advice, and training are in place to support the CoP's implementation and compliance, and for ensuring these artifacts are regularly reviewed at appropriate intervals.

23. Mobile Device owners are responsible for ensuring that the requirements of this CoP are enforced when using relevant devices.

References and Associated Documentation (Legislation, Other Policies, other parties)

24. This CoP forms part of a suite of related Information Security documents.

OPERATIONAL APPLICATION

Device Eligibility

25. Only approved mobile devices that meet the university's security requirements are permitted to access university systems and data.

26. Approved devices must support the required security controls. Digital Services will maintain a list of approved devices and operating systems.

Security Requirements

27. All mobile devices must be encrypted to protect university data.

28. Where possible to configure, mobile devices must be protected by a physical or software firewall.

29. Devices must be protected by strong passwords or biometric authentication.

30. Mobile device operating systems, firmware and installed software must be patched and up to date with the latest security updates installed. Critical security patches must be applied within 14 days of release.

31. Updates, patches and other system settings must be applied automatically where possible.

32. Mobile devices used to access University IT systems and services that are at risk of malware infection must run AV (anti-virus) software that is continuously updated.

33. Anti-Virus software must be configured to perform real-time scanning and periodic full system scans, including scans for potentially malicious websites and warnings against accessing them.

34. Mobile devices allowing access to important, sensitive, or critical information must not be left unattended.

35. Users must not attempt to bypass or remove device restrictions and security controls imposed either by the manufacturer or by the university. This includes any attempt to "root" or "jailbreak" devices to allow the installation of unapproved or unauthorised software, firmware, or unsigned applications, or to gain access to functionality not intended to be exposed to the user.

36. Auto-run or auto-play functionality on BYOD must be turned off to avoid the unintended installation or triggering of malicious software

Access Control

37. Mobile devices must require authentication via password or PIN to access. These must meet any complexity requirements set out by the University.

38. Remote access to university systems must be via the university approved secure Virtual Private Network (VPN).

39. Multi-factor authentication (MFA) must be used when accessing the University IT Environment remotely.

40. The use of unprotected public Wi-Fi for accessing the University IT Environment must be avoided.

41. If a domestic wireless solution is used at the user's premises, it must be made secure, utilising the wireless security features and password included with the wireless solution, to ensure no unauthorised access is permitted.

42. Default passwords for admin and/or users accounts on BYOD must be changed to meet the any complexity requirements set out by the University.

43. Multi-factor authentication (MFA) must be enabled for accessing sensitive systems and data.

44. Users must prevent access to anyone else except the individual who is designated as the mobile device owner.

Data Protection

45. Use of local storage on mobile devices as primary repositories of sensitive university data must be avoided. Approved, secure cloud storage solutions provided by the university should be used.

46. If it is unavoidable, University data stored locally on mobile devices must be encrypted both in transit and at rest. This includes using secure communication protocols (minimum TLS 1.2) and device encryption.

47. Individuals using mobile devices must seek guidance from digital services if they are unsure about the back-up arrangements for any data.

48. When using mobile devices in public places, the user must take care that data cannot be read by unauthorised persons.

User Responsibilities

49. If a domestic wireless solution is used at the user's premises, it must be made secure utilising the wireless security features and password included with the wireless solution, to ensure no unauthorised access is permitted.

50. The use of software applications on mobile devices for processing university data must be appropriate to the license under which they are used.

51. The physical security of mobile devices must be maintained when used outside of University premises. Devices must not be left unattended in unsecured areas.

52. Any potential data breach, loss or compromise of commercially sensitive data, or suspected cyber incident involving mobile devices, should be reported via the university's incident reporting process. If unsure contact the Service Desk.

53. Users must comply with any requirements of the University in relation to mobile devices that are owned or have been procured or configured by the University.

54. Users must return mobile devices to the University when they are no longer required, or when their relationship with the University ends.

Monitoring and Auditing

55. The university reserves the right to monitor the use of mobile devices to ensure compliance with this policy.

56. Monitoring may include reviewing access logs, conducting security assessments, and auditing device configurations. Users will be notified of any monitoring activities.

57. Regular audits will be conducted to ensure compliance with this CoP and identify any security risks.

58. Audits will include reviewing device registrations, access logs, and security configurations. Any non-compliance issues will be addressed promptly.

Termination of Access

59. The university reserves the right to revoke access to university systems and data from mobile devices at any time.

60. Access may be revoked for non-compliance with this CoP, security concerns, or changes in user roles. Users will be notified of any access revocations.

61. If required, Digital Services will assist users in securely removing university data from their devices. Users must confirm that all data has been removed.

COP MANAGEMENT

CoP Review

62. This CoP will be reviewed every two years. It is the responsibility of the Head of Cyber Security to ensure that these reviews take place and remains internally consistent.

63. Reviews resulting in minor changes shall be signed off by the Director of Digital Services prior to deployment. Substantial changes to the CoP shall be approved by the Digital Services Senior Management Board prior to deployment.

64. Substantive changes to this CoP shall be communicated to all relevant Users.

CoP Specifications

Organisation	Leeds Beckett University
Author(s)	Dominic Jennings (Cyber Security Assurance Analyst)
Developed in consultation with	Digital Services, Cyber Security, Information Governance, Registrar & Secretary's Office
Owner	Director of Digital Services
Target audience	All staff, students and all other relevant parties
Sensitivity	Public
EDI Assessment	The policy supports the principles of the university's approach to IT and Cyber Security and includes a commitment to complying with legal and regulatory requirements by adhering to applicable UK laws and regulations ensuring fair, transparent and equal implementation of controls. No significant EDI impacts have been identified. The CoP will continue to be monitored to ensure fairness, transparency, and equality of treatment for all users
Approved by	Director of Digital Services
Endorsed by	Digital Services Management Board
Effective from	11-04-2026

Last review date	11-04-2026
Next review date	+2 years from last date of approval [04-2028]
Status	**Published**
Distribution	All Services, Staff, Teams, and Users.
External references	None
Links to other internal policies / procedures	University policies | Leeds Beckett University
Version reference	1.0
Version History - summary of changes (inc. committee paper reference if applicable)	New CoP. Supersedes previous CoP/guidance contained in IT Security Policies.